

CODES ASSOCIATED WITH $O(3, 2^r)$ AND POWER MOMENTS OF KLOOSTERMAN SUMS WITH TRACE ONE ARGUMENTS

DAE SAN KIM

ABSTRACT. We construct a binary linear code $C(O(3, q))$, associated with the orthogonal group $O(3, q)$. Here q is a power of two. Then we obtain a recursive formula for the odd power moments of Kloosterman sums with trace one arguments in terms of the frequencies of weights in the codes $C(O(3, q))$ and $C(Sp(2, q))$. This is done via Pless power moment identity and by utilizing the explicit expressions of Gauss sums for the orthogonal groups.

1. INTRODUCTION

Let ψ be a nontrivial additive character of the finite field \mathbb{F}_q with $q = p^r$ elements (p a prime). Then the Kloosterman sum $K(\psi; a)$ ([10]) is defined by

$$K(\psi; a) = \sum_{\alpha \in \mathbb{F}_q^*} \psi(\alpha + a\alpha^{-1}) (a \in \mathbb{F}_q^*).$$

The Kloosterman sum was introduced in 1926([9]) to give an estimate for the Fourier coefficients of modular forms.

For each nonnegative integer h , we denote by $MK(\psi)^h$ the h -th moment of the Kloosterman sum $K(\psi; a)$, i.e.,

$$MK(\psi)^h = \sum_{a \in \mathbb{F}_q^*} K(\psi; a)^h.$$

If $\psi = \lambda$ is the canonical additive character of \mathbb{F}_q , then $MK(\lambda)^h$ will be simply denoted by MK^h .

Also, we introduce two incomplete power moments of Kloosterman sums, namely the one with the sum over all a in \mathbb{F}_q^* with $tra = 0$ and the other with the sum over all a in \mathbb{F}_q^* with $tra = 1$. For every nonnegative integer h , and ψ as before, we define

$$(1) \quad T_0 K(\psi)^h = \sum_{a \in \mathbb{F}_q^*, tra=0} K(\psi; a)^h, \quad T_1 K(\psi)^h = \sum_{a \in \mathbb{F}_q^*, tra=1} K(\psi; a)^h,$$

2000 *Mathematics Subject Classification.* MSC 2000: 11T23, 20G40, 94B05.

This work was supported by National Research Foundation of Korea Grant funded by the Korean Government 2009-0072514.

which will be respectively called the h -th moment of Kloosterman sums with “trace zero arguments” and that with “trace one arguments.” Then, clearly we have

$$(2) \quad MK(\psi)^h = T_0K(\psi)^h + T_1K(\psi)^h.$$

If $\psi = \lambda$ is the canonical additive character of \mathbb{F}_q , then $T_0K(\lambda)^h$ and $T_1K(\lambda)^h$ will be respectively denoted by T_0K^h and T_1K^h , for brevity.

Explicit computations on power moments of Kloosterman sums were initiated in the paper [15] of Salié in 1931, where it is shown that for any odd prime q ,

$$MK^h = q^2M_{h-1} - (q-1)^{h-1} + 2(-1)^{h-1} \quad (h \geq 1).$$

Here $M_0 = 0$, and, for $h \in \mathbb{Z}_{>0}$,

$$M_h = |\{(\alpha_1, \dots, \alpha_h) \in (\mathbb{F}_q^*)^h \mid \sum_{j=1}^h \alpha_j = 1 = \sum_{j=1}^h \alpha_j^{-1}\}|.$$

For $q = p$ an odd prime, Salié obtained MK^1, MK^2, MK^3, MK^4 in [15] by determining MK^1, MK^2, MK^3 . MK^5 can be expressed in terms of the p -th eigenvalue for a weight 3 newform on $\Gamma_0(15)$ (cf. [11], [14]). MK^6 can be expressed in terms of the p -th eigenvalue for a weight 4 newform on $\Gamma_0(6)$ (cf. [3]). Also, based on numerical evidence, in [2] Evans was led to propose a conjecture which expresses MK^7 in terms of Hecke eigenvalues for a weight 3 newform on $\Gamma_0(525)$ with quartic nebentypus of conductor 105.

From now on, let us assume that $q = 2^r$. Carlitz[1] evaluated MK^h for $h \leq 4$. Recently, Moisiu was able to find explicit expressions of MK^h , for $h \leq 10$ (cf. [13]). This was done, via Pless power moment identity, by connecting moments of Kloosterman sums and the frequencies of weights in the binary Zetterberg code of length $q+1$, which were known by the work of Schoof and Vlught in [16].

In this paper, we will show the main Theorem 1.1 giving a recursive formula for the odd power moments of Kloosterman sums with trace one arguments. To do that, we construct a binary linear code $C(O(3, q))$, associated with the orthogonal group $O(3, q)$, and express those power moments in terms of the frequencies of weights in the codes $C(O(3, q))$ and $C(Sp(2, q))$. Here $C(Sp(2, q))$ is a binary linear code associated with the symplectic group $Sp(2, q)$ (cf. [7]). Then, thanks to our previous results on the explicit expressions of “Gauss sums” for the orthogonal group $O(2n+1, q)$ [8], we can express the weight of each codeword in the dual of the code in terms of Kloosterman sums. Then our formula will follow immediately from the Pless power moment identity. The reader is referred to [5] for the construction of code associated with other type of orthogonal group and the derivation of recursive formulas generating power moments of Kloosterman sums.

In [7], for both n, q powers of two, a binary linear code $C(SL(n, q))$ associated with the finite special linear group $SL(n, q)$ was constructed in order to produce a recursive formula for the power moments of multi-dimensional Kloosterman sums in terms of the frequencies of weights in that code. On the other hand, in [6], for q a power of three, two infinite families of ternary linear codes associated with double cosets in the symplectic group $Sp(2n, q)$ were constructed in order to generate infinite families of recursive formulas for the power moments of Kloosterman sums with square arguments and for the even power moments of those in terms of the frequencies of weights in those codes.

Henceforth, we agree that the binomial coefficient $\binom{b}{a} = 0$, if $a > b$ or $a < 0$.

Theorem 1.1. *Let $q = 2^r$. Then we have the following. For $h = 1, 3, 5, \dots$,*

$$(3) \quad T_1 K^h = - \sum_{1 \leq j \leq h-2, j \text{ odd}} \binom{h}{j} (q^2 - 1)^{h-j} T_1 K^j \\ + q^{1-h} \sum_{j=0}^{\min\{N, h\}} (-1)^j D_j \sum_{t=j}^h t! S(h, t) 2^{h-t-1} \binom{N-j}{N-t},$$

where $N = |O(3, q)| = q(q^2 - 1)$, and $D_j = C_j - \hat{C}_j$ ($0 \leq j \leq N$), with $\{C_j\}_{j=0}^N, \{\hat{C}_j\}_{j=0}^N$ respectively the weight distributions of $C(O(3, q))$ and $C(Sp(2, q))$ given by: for $j = 0, \dots, N$,

$$(4) \quad C_j = \sum \binom{q^2}{\nu_1} \prod_{\text{tr}((\beta-1)^{-1})=0} \binom{q^2+q}{\nu_\beta} \prod_{\text{tr}((\beta-1)^{-1})=1} \binom{q^2-q}{\nu_\beta},$$

$$(5) \quad \hat{C}_j = \sum \binom{q^2}{\nu_0} \prod_{\text{tr}(\beta^{-1})=0} \binom{q^2+q}{\nu_\beta} \prod_{\text{tr}(\beta^{-1})=1} \binom{q^2-q}{\nu_\beta}.$$

Here the first sum in (3) is 0 if $h = 1$ and the unspecified sums in (4) and (5) run over all the sets of nonnegative integers $\{\nu_\beta\}_{\beta \in \mathbb{F}_q}$ satisfying $\sum_{\beta \in \mathbb{F}_q} \nu_\beta = j$ and $\sum_{\beta \in \mathbb{F}_q} \nu_\beta \beta = 0$. In addition, $S(h, t)$ is the Stirling number of the second kind defined by

$$(6) \quad S(h, t) = \frac{1}{t!} \sum_{j=0}^t (-1)^{t-j} \binom{t}{j} j^h.$$

2. $O(2n+1, q)$

For more details about this section, one is referred to the paper [8]. Throughout this paper, the following notations will be used:

$$q = 2^r \ (r \in \mathbb{Z}_{>0}),$$

\mathbb{F}_q = the finite field with q elements,

TrA = the trace of A for a square matrix A ,

tB = the transpose of B for any matrix B .

Let θ be the nondegenerate quadratic form on the vector space $\mathbb{F}_q^{(2n+1) \times 1}$ of all $(2n+1) \times 1$ column vectors over \mathbb{F}_q , given by

$$\theta\left(\sum_{i=1}^{2n+1} x_i e^i\right) = \sum_{i=1}^n x_i x_{n+i} + x_{2n+1}^2,$$

where $\{e^1 = {}^t[10 \dots 0], e^2 = {}^t[010 \dots 0], \dots, e^{2n+1} = {}^t[0 \dots 01]\}$ is the standard basis of $\mathbb{F}_q^{(2n+1) \times 1}$.

The group $O(2n+1, q)$ of all isometries of $(\mathbb{F}_q^{(2n+1) \times 1}, \theta)$ consists of the matrices

$$\begin{bmatrix} A & B & 0 \\ C & D & 0 \\ g & h & 1 \end{bmatrix} \quad (A, B, C, D \ n \times n, g, h \ 1 \times n)$$

in $GL(2n+1, q)$ satisfying the relations:

$$\begin{aligned} {}^tAC + {}^tgg & \text{ is alternating,} \\ {}^tBD + {}^thh & \text{ is alternating,} \\ {}^tAD + {}^tCB & = 1_n. \end{aligned}$$

Here an $n \times n$ matrix (a_{ij}) is called alternating if

$$\begin{cases} a_{ii} = 0, & \text{for } 1 \leq i \leq n, \\ a_{ij} = -a_{ji} = a_{ji}, & \text{for } 1 \leq i < j \leq n. \end{cases}$$

Also, one observes, for example, that ${}^tAC + {}^tgg$ is alternating if and only if ${}^tAC = {}^tCA$ and $g = \sqrt{\text{diag}({}^tAC)}$, where $\sqrt{\text{diag}({}^tAC)}$ indicates the $1 \times n$ matrix $[\alpha_1, \dots, \alpha_n]$ if the diagonal entries of tAC are given by

$$({}^tAC)_{11} = \alpha_1^2, \dots, ({}^tAC)_{nn} = \alpha_n^2, \text{ for } \alpha_i \in \mathbb{F}_q.$$

As is well known, there is an isomorphism of groups

$$(7) \quad \iota : O(2n+1, q) \rightarrow Sp(2n, q) \quad \left(\begin{bmatrix} A & B & 0 \\ C & D & 0 \\ g & h & 1 \end{bmatrix} \mapsto \begin{bmatrix} A & B \\ C & D \end{bmatrix} \right).$$

In particular, for any $w \in O(2n+1, q)$,

$$(8) \quad Trw = Tr\iota(w) + 1.$$

Here the symplectic group $Sp(2n, q)$ over the field \mathbb{F}_q is defined as:

$$Sp(2n, q) = \{w \in GL(2n, q) \mid {}^t w J w = J\},$$

with

$$J = \begin{bmatrix} 0 & 1_n \\ 1_n & 0 \end{bmatrix}.$$

$$(9) \quad |O(2n+1, q)| = |Sp(2n, q)| = q^{n^2} \prod_{j=1}^n (q^{2j} - 1) \quad (\text{cf. (7), [4]}).$$

For integers n, r with $0 \leq r \leq n$, the q -binomial coefficients are defined as:

$$(10) \quad \begin{bmatrix} n \\ r \end{bmatrix}_q = \prod_{j=0}^{r-1} (q^{n-j} - 1) / (q^{r-j} - 1).$$

3. GAUSS SUMS FOR $O(2n+1, q)$

The following notations will be used throughout this paper.

$tr(x) = x + x^2 + \cdots + x^{2^{r-1}}$ the trace function $\mathbb{F}_q \rightarrow \mathbb{F}_2$,

$\lambda(x) = (-1)^{tr(x)}$ the canonical additive character of \mathbb{F}_q .

Then any nontrivial additive character ψ of \mathbb{F}_q is given by $\psi(x) = \lambda(ax)$, for a unique $a \in \mathbb{F}_q^*$.

For any nontrivial additive character ψ of \mathbb{F}_q and $a \in \mathbb{F}_q^*$, the Kloosterman sum $K_{GL(t, q)}(\psi; a)$ for $GL(t, q)$ is defined as

$$(11) \quad K_{GL(t, q)}(\psi; a) = \sum_{w \in GL(t, q)} \psi(Trw + a Trw^{-1}).$$

Observe that, for $t = 1$, $K_{GL(1, q)}(\psi; a)$ denotes the Kloosterman sum $K(\psi; a)$.

In [4], it is shown that $K_{GL(t, q)}(\psi; a)$ satisfies the following recursive relation: for integers $t \geq 2$, $a \in \mathbb{F}_q^*$,

$$(12) \quad K_{GL(t, q)}(\psi; a) = q^{t-1} K_{GL(t-1, q)}(\psi; a) K(\psi; a) \\ + q^{2t-2} (q^{t-1} - 1) K_{GL(t-2, q)}(\psi; a),$$

where we understand that $K_{GL(0,q)}(\psi; a) = 1$.

From [4] and [8], the Gauss sum for $O(2n+1, q)$ is equal to $\psi(1)$ times that for $Sp(2n, q)$ and is given by (cf. (10), (11)):

$$\begin{aligned} \sum_{w \in O(2n+1, q)} \psi(Trw) &= \psi(1) \sum_{w \in Sp(2n, q)} \psi(Trw) \\ &= \psi(1) q^{\binom{n+1}{2}} \sum_{0 \leq r \leq n, \text{ } r \text{ even}} q^{rn - \frac{1}{4}r^2} \begin{bmatrix} n \\ r \end{bmatrix}_q \prod_{j=1}^{r/2} (q^{2j-1} - 1) K_{GL(n-r, q)}(\psi; 1). \end{aligned}$$

Here ψ is any nontrivial additive character of \mathbb{F}_q . For our purposes, we only need the following expression of the Gauss sum for $O(3, q)$. So we state it separately as a theorem.

Theorem 3.1. *Let ψ be any nontrivial additive character of \mathbb{F}_q . Then we have*

$$\sum_{w \in O(3, q)} \psi(Trw) = \psi(1) q K(\psi; 1).$$

Proposition 3.2. ([5]) *For $n = 2^s$ ($s \in \mathbb{Z}_{\geq 0}$), and λ the canonical additive character of \mathbb{F}_q ,*

$$K(\lambda; a^n) = K(\lambda; a).$$

The next corollary follows from Theorem 2 and Proposition 3 and by simple change of variables.

Corollary 3.3. *Let λ be the canonical additive character of \mathbb{F}_q , and let $a \in \mathbb{F}_q^*$. Then we have*

$$(13) \quad \sum_{w \in O(3, q)} \lambda(aTrw) = \lambda(a) q K(\lambda; a).$$

Proposition 3.4. ([5]) *Let λ be the canonical additive character of \mathbb{F}_q , $\beta \in \mathbb{F}_q$. Then*

$$\begin{aligned} (14) \quad & \sum_{a \in \mathbb{F}_q^*} \lambda(-a\beta) K(\lambda; a) \\ &= \begin{cases} q\lambda(\beta^{-1}) + 1, & \text{if } \beta \neq 0, \\ 1, & \text{if } \beta = 0. \end{cases} \end{aligned}$$

Let $G(q)$ be one of finite classical groups over \mathbb{F}_q . Then we put, for each $\beta \in \mathbb{F}_q$,

$$N_{G(q)}(\beta) = |\{w \in G(q) | Tr(w) = \beta\}|.$$

Then it is easy to see that

$$(15) \quad qN_{G(q)}(\beta) = |G(q)| + \sum_{a \in \mathbb{F}_q^*} \lambda(-a\beta) \sum_{w \in G(q)} \lambda(aTrw).$$

For brevity, we write

$$(16) \quad n(\beta) = N_{O(3,q)}(\beta).$$

Using (13)-(15), one derives the following.

Proposition 3.5. *We have*

$$(17) \quad n(\beta) = \begin{cases} q^2, & \text{if } \beta = 1, \\ q^2 + q, & \text{if } tr((\beta - 1)^{-1}) = 0, \\ q^2 - q, & \text{if } tr((\beta - 1)^{-1}) = 1. \end{cases}$$

Corollary 3.6. *$Tr : O(3, q) \rightarrow \mathbb{F}_q$ is surjective.*

Proof. From (17), we see that $n(\beta) > 0$, for all $\beta \in \mathbb{F}_q$. Alternatively, this also follows from the easily shown surjectivity of $Tr : Sp(2n, q) \rightarrow \mathbb{F}_q$ and the facts in (7) and (8). \square

In below, “the sum over $tra = 0$ ” will mean “the sum over all nonzero $a \in \mathbb{F}_q^*$, with $tra = 0$.”

The result (b) in below and hence (a) follow also from (3).

Proposition 3.7. *Let $q = 2^r$. Then we have the following.*

$$(a) \quad T_0K = 1 + \frac{1}{2}(-1)^r q.$$

$$(b) \quad T_1K = \frac{1}{2}(-1)^{r+1} q.$$

Proof. (a)

$$\begin{aligned} T_0K &= \sum_{tra=0} \sum_{x \in \mathbb{F}_q^*} \lambda(x + ax^{-1}) \\ &= \sum_{tra=0} \sum_{x \in \mathbb{F}_q^*} \lambda(x^{-1} + ax) \\ &= \frac{1}{2} \sum_{x \in \mathbb{F}_q^*} \lambda(x^{-1}) \sum_{\alpha \in \mathbb{F}_q \setminus \{0,1\}} \lambda((\alpha^2 + \alpha)x) \\ &= \frac{1}{2} \sum_{x \in \mathbb{F}_q^*} \lambda(x^{-1}) \left\{ \sum_{\alpha \in \mathbb{F}_q} \lambda(x\alpha^2 + x\alpha) - 2 \right\} \\ (18) \quad &= 1 + \frac{1}{2} \sum_{x \in \mathbb{F}_q^*} \lambda(x^{-1}) \sum_{\alpha \in \mathbb{F}_q} \lambda(x\alpha^2 + x\alpha). \end{aligned}$$

Now, from Theorem 5.34 of [10], we have

$$\sum_{\alpha \in \mathbb{F}_q} \lambda(x\alpha^2 + x\alpha) = \begin{cases} q, & \text{if } x^2 + x = 0 \text{ (i.e., } x \in \mathbb{F}_2), \\ 0, & \text{otherwise.} \end{cases}$$

Thus (18) equals

$$1 + \frac{q}{2} \sum_{x \in \mathbb{F}_2^*} \lambda(x^{-1}) = 1 + \frac{1}{2}(-1)^r q.$$

(b) This follows from (a), since $T_1 K = MK - T_0 K = 1 - T_0 K$. \square

4. CONSTRUCTION OF CODES

Let

$$(19) \quad N = |O(3, q)| = q(q^2 - 1).$$

Here we will construct a binary linear code $C(O(3, q))$ of length N , associated with the orthogonal group $O(3, q)$.

Let g_1, g_2, \dots, g_N be a fixed ordering of the elements in the group $O(3, q)$. Also, we put

$$v = (Tr g_1, Tr g_2, \dots, Tr g_N) \in \mathbb{F}_q^N.$$

Then the binary linear code $C(O(3, q))$ is defined as

$$(20) \quad C(O(3, q)) = \{u \in \mathbb{F}_2^N \mid u \cdot v = 0\},$$

where the dot denotes the usual inner product in \mathbb{F}_q^N .

The following Delsarte's theorem is well-known.

Theorem 4.1. ([12]) *Let B be a linear code over \mathbb{F}_q . Then*

$$(B|_{\mathbb{F}_2})^\perp = tr(B^\perp).$$

In view of this theorem, the dual $C(O(3, q))^\perp$ is given by

$$(21) \quad C(O(3, q))^\perp = \{c(a) = (tr(aTr g_1), \dots, tr(aTr g_N)) \mid a \in \mathbb{F}_q\}.$$

Proposition 4.2. *For every $q = 2^r$, the map $\mathbb{F}_q \rightarrow C(O(3, q))^\perp$ ($a \mapsto c(a)$) is an \mathbb{F}_2 -linear isomorphism.*

Proof. The map is clearly \mathbb{F}_2 -linear and surjective. Let a be in the kernel of the map. Then, in view of Corollary 3.6, $tr(\alpha\beta) = 0$, for all $\beta \in \mathbb{F}_q$. Since the trace function $\mathbb{F}_q \rightarrow \mathbb{F}_2$ is surjective, $a = 0$. \square

5. POWER MOMENTS OF KLOOSTERMAN SUMS WITH TRACE ONE ARGUMENTS

In this section, we will be able to find, via Pless power moment identity, a recursive formula for the power moments of Kloosterman sums with trace one arguments in terms of the frequencies of weights in the codes $C(O(3, q))$ and $C(Sp(2, q))$.

Theorem 5.1. (*Pless power moment identity*) Let B be an q -ary $[n, k]$ code, and let B_i (resp. B_i^\perp) denote the number of codewords of weight i in B (resp. in B^\perp). Then, for $h = 0, 1, 2, \dots$,

$$(22) \quad \sum_{j=0}^n j^h B_j = \sum_{j=0}^{\min\{n, h\}} (-1)^j B_j^\perp \sum_{t=j}^h t! S(h, t) q^{k-t} (q-1)^{t-j} \binom{n-j}{n-t},$$

where $S(h, t)$ is the Stirling number of the second kind defined in (6).

Lemma 5.2. Let $c(a) = (tr(aTrg_1), \dots, tr(aTrg_N)) \in C(O(3, q))^\perp$, for $a \in \mathbb{F}_q^*$. Then the Hamming weight $w(c(a))$ can be expressed as follows:

$$(23) \quad w(c(a)) = \frac{1}{2} q \{ (q^2 - 1) - \lambda(a) K(\lambda; a) \}.$$

Proof.

$$\begin{aligned} w(c(a)) &= \frac{1}{2} \sum_{j=1}^N (1 - (-1)^{tr(aTrg_j)}) \\ &= \frac{1}{2} (N - \sum_{w \in O(3, q)} \lambda(aTrw)). \end{aligned}$$

Our results now follow from (19) and (13). \square

Let $u = (u_1, \dots, u_N) \in \mathbb{F}_2^N$, with ν_β 1's in the coordinate places where $Tr(g_j) = \beta$, for each $\beta \in \mathbb{F}_q$. Then we see from the definition of the code $C(O(3, q))$ (cf. (20)) that u is a codeword with weight j if and only if $\sum_{\beta \in \mathbb{F}_q} \nu_\beta = j$ and $\sum_{\beta \in \mathbb{F}_q} \nu_\beta \beta = 0$ (an identity in \mathbb{F}_q). Note that there are $\prod_{\beta \in \mathbb{F}_q} \binom{n(\beta)}{\nu_\beta}$ many such codewords with weight j . Now, we obtain the following formula in (24), by using the explicit value of $n(\beta)$ in (17).

Theorem 5.3. Let $q = 2^r$ be as before, and let $\{C_j\}_{j=0}^N$ be the weight distribution of $C(O(3, q))$. Then, for $j = 0, \dots, N$,

$$(24) \quad C_j = \sum \binom{q^2}{\nu_1} \prod_{tr((\beta-1)^{-1})=0} \binom{q^2+q}{\nu_\beta} \prod_{tr((\beta-1)^{-1})=1} \binom{q^2-q}{\nu_\beta},$$

where the sum runs over all the sets of nonnegative integers $\{\nu_\beta\}_{\beta \in \mathbb{F}_q}$ satisfying

$$(25) \quad \sum_{\beta \in \mathbb{F}_q} \nu_\beta = j \quad \text{and} \quad \sum_{\beta \in \mathbb{F}_q} \nu_\beta \beta = 0,$$

and the first and second products are over all $\beta \neq 1$, respectively with $tr((\beta-1)^{-1}) = 0$ and $tr((\beta-1)^{-1}) = 1$.

Corollary 5.4. *Let $\{C_j\}_{j=0}^N$ be the weight distribution of $C(O(3, q))$. Then we have $C_j = C_{N-j}$, for all j , with $0 \leq j \leq N$.*

Proof. Under the replacements $\nu_\beta \rightarrow n(\beta) - \nu_\beta$, for each $\beta \in \mathbb{F}_q$, the first equation in (25) is changed to $N - j$, while the second one in (25) and the summands in (24) are left unchanged. Here the second sum in (25) is left unchanged, since $\sum_{\beta \in \mathbb{F}_q} n(\beta)\beta = 0$, as one can see by using the explicit expression of $n(\beta)$ in (17). \square

The recursive formula in the following theorem follows from the study of codes associated with symplectic group $Sp(2, q) = SL(2, q)$. They are slightly modified from their original versions, which makes them more usable in below.

Theorem 5.5. ([7]) *For $h = 1, 2, 3, \dots$,*

$$(26) \quad \begin{aligned} & \left(\frac{q}{2}\right)^h \sum_{j=0}^h (-1)^j \binom{h}{j} (q^2 - 1)^{h-j} MK^j \\ &= q \sum_{j=0}^{\min\{N, h\}} (-1)^j \hat{C}_j \sum_{t=j}^h t! S(h, t) 2^{-t} \binom{N-j}{N-t}, \end{aligned}$$

where $N = q(q^2 - 1) = |Sp(2, q)| = |O(3, q)|$, $S(h, t)$ indicates the Stirling number of the second kind as in (6), and $\{\hat{C}_j\}_{j=0}^N$ denotes the weight distribution of the code $C(Sp(2, q))$, given by

$$\hat{C}_j = \sum \binom{q^2}{\nu_0} \prod_{\text{tr}(\beta^{-1})=0} \binom{q^2+q}{\nu_\beta} \prod_{\text{tr}(\beta^{-1})=1} \binom{q^2-q}{\nu_\beta} \quad (0 \leq j \leq N).$$

Here the sum runs over all the sets of nonnegative integers $\{\nu_\beta\}_{\beta \in \mathbb{F}_q}$ satisfying $\sum_{\beta \in \mathbb{F}_q} \nu_\beta = j$ and $\sum_{\beta \in \mathbb{F}_q} \nu_\beta \beta = 0$, and the first and second product run over the elements $\beta \in \mathbb{F}_q^*$, respectively with $\text{tr}(\beta^{-1}) = 0$ and $\text{tr}(\beta^{-1}) = 1$.

We are now ready to apply the Pless power moment identity in (22) to $C(O(3, q))^\perp$, in order to obtain the result in Theorem 1.1 (cf. (3)) about a recursive formula.

Then the left hand side of that identity in (22) is equal to

$$(27) \quad \sum_{a \in F_q^*} w(c(a))^h,$$

with the $w(c(a))$ given by (23).

(27) is now given by

$$\begin{aligned}
& \left(\frac{q}{2}\right)^h \sum_{a \in \mathbb{F}_q^*} (q^2 - 1 - \lambda(a)K(\lambda; a))^h \\
&= \left(\frac{q}{2}\right)^h \sum_{tra=0} (q^2 - 1 - K(\lambda; a))^h + \left(\frac{q}{2}\right)^h \sum_{tra=1} (q^2 - 1 + K(\lambda; a))^h \\
&= \left(\frac{q}{2}\right)^h \sum_{tra=0} \sum_{j=0}^h (-1)^j \binom{h}{j} (q^2 - 1)^{h-j} (K(\lambda; a))^j \\
&\quad + \left(\frac{q}{2}\right)^h \sum_{tra=1} \sum_{j=0}^h \binom{h}{j} (q^2 - 1)^{h-j} (K(\lambda; a))^j \\
&= \left(\frac{q}{2}\right)^h \sum_{j=0}^h (-1)^j \binom{h}{j} (q^2 - 1)^{h-j} (MK^j - T_1 K^j) \quad (\psi = \lambda \text{ case of (1), (2)}) \\
&\quad + \left(\frac{q}{2}\right)^h \sum_{j=0}^h \binom{h}{j} (q^2 - 1)^{h-j} T_1 K^j \\
&= \left(\frac{q}{2}\right)^h \sum_{j=0}^h (-1)^j \binom{h}{j} (q^2 - 1)^{h-j} MK^j \\
&\quad + 2 \left(\frac{q}{2}\right)^h \sum_{0 \leq j \leq h, j \text{ odd}} \binom{h}{j} (q^2 - 1)^{h-j} T_1 K^j \\
(28) \quad &= q \sum_{j=0}^{\min\{N, h\}} (-1)^j \hat{C}_j \sum_{t=j}^h t! S(h, t) 2^{-t} \binom{N-j}{N-t} \quad (\text{cf. (26)}) \\
&\quad + 2 \left(\frac{q}{2}\right)^h \sum_{0 \leq j \leq h, j \text{ odd}} \binom{h}{j} (q^2 - 1)^{h-j} T_1 K^j.
\end{aligned}$$

Here one has to separate the term corresponding to $l = h$ in (28), and note $\dim_{\mathbb{F}_2} C(O(3, q)) = r$.

REFERENCES

- [1] L. Carlitz, ‘Gauss sums over finite fields of order 2^n ,’ *Acta Arith.* **15** (1969), 247-265.
- [2] R.J.Evans, ‘Seventh power moments of Kloosterman sums,’ *Israel J. Math.*, to appear.
- [3] K. Hulek, J. Spandaw, B. van Geemen, and D. van Straten, ‘The modularity of the Barth-Nieto quintic and its relatives,’ *Adv. Geom.* **1** (2001), 263-289.
- [4] D. S. Kim, ‘Gauss sums for symplectic groups over a finite field,’ *Mh. Math.* **126** (1998), 55-71.
- [5] D. S. Kim, ‘Codes associated with $O^+(2n, 2^r)$ and power moments of Kloosterman sums,’ submitted.

- [6] D. S. Kim, *Infinite families of recursive formulas generating power moments of ternary Kloosterman sums with square arguments arising from symplectic groups*, Adv. Math. Commun. **3**(2009), 167–178.
- [7] D. S. Kim, *Codes associated with special linear groups and power moments of multi-dimensional Kloosterman sums*, Ann. Mat. Pura Appl. **190**(2011), 61–76.
- [8] D. S. Kim and Y. H. Park, ‘Gauss sums for orthogonal groups over a finite field of characteristic two,’ *Acta Arith.* **82** (1997), 331–357.
- [9] H. D. Kloosterman, ‘On the representation of numbers in the form $ax^2 + by^2 + cz^2 + dt^2$,’ *Acta Math.* **49** (1926), 407–464.
- [10] R. Lidl and H. Niederreiter, *Finite Fields*, (Encyclopedia Math. Appl. 20)(Cambridge Univ. Press, Cambridge and New York, 1987).
- [11] R. Livné, ‘Motivic orthogonal two-dimensional representations of $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$,’ *Israel J. Math.* **92** (1995), 149–156.
- [12] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error Correcting Codes*, (North-Holland, Amsterdam, 1998).
- [13] M. Moisio, ‘The moments of a Kloosterman sum and the weight distribution of a Zetterberg-type binary cyclic code,’ *IEEE Trans. Inform. Theory* **53** (2007), 843–847.
- [14] C. Peters, J. Top, and M. van der Vlugt, ‘Über die Kloostermanschen Summen $S(u, v; q)$,’ *Math. Z.* **34** (1931), 91–109.
- [15] H. Salié, ‘The Hasse zeta function of a $K3$ surface related to the number of words of weight 5 in the Melas codes,’ *J. Reine Angew. Math.* **432** (1992), 151–176.
- [16] R. Schoof and M. van der Vlugt, ‘Hecke operators and the weight distributions of certain codes,’ *J. Combin. Theory Ser. A* **57** (1991), 163–186.

DEPARTMENT OF MATHEMATICS, SOGANG UNIVERSITY, SEOUL 121-742, KOREA

E-mail address: dskim@sogang.ac.kr